[F1[F2ANNEX I B U.K.

REQUIREMENTS FOR CONSTRUCTION, TESTING, INSTALLATION AND INSPECTION

Textual Amendments

F1 Inserted by Council Regulation (EC) No 2135/98 of 24 September 1998 amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/85 and (EEC) No 3821/85.

F2 Substituted by Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport (Text with EEA relevance).

Appendix 10 U.K.

GENERIC SECURITY TARGETS

TACHOGRAPH CARD GENERIC SECURITY TARGET

1. Introduction U.K.

This document contains a description of the tachograph card, of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the required security enforcing functions. It states the claimed minimum strength of security mechanisms, and the required level of assurance for the development and the evaluation.

Requirements referred to in the document, are those of the body of Annex I B. For clarity of reading, duplication sometimes arises between Annex I B body requirements and security target requirements. In case of ambiguity between a security target requirement and the Annex I B requirement referred by this security target requirement, the Annex I B body requirement shall prevail.

Annex I B body requirements not referred by security targets are not the subject of security enforcing functions.

A tachograph card is a standard smart card carrying a dedicated tachograph application, and shall comply with up-to-date functional and assurance security requirements applicable to smart cards. This security target therefore incorporates only the extra security requirements needed by the tachograph application.

Unique labels have been assigned to threats, objectives, procedural means and SEF specifications for the purpose of traceability to development and evaluation documentation.

2. Abbreviations, definitions and references U.K.

2.1. Abbreviations U.K.

IC	Integrated Circuit (electronic component designed to perform processing and/or memory functions)
OS	Operating system
PIN	Personal identification number
ROM	Read only memory
SFP	Security functions policy
TBD	To be defined
TOE	Target of evaluation
TSF	TOE security function
VU	Vehicle unit.

2.2. Definitions U.K.

Digital tachograph Recording equipment.

Sensitive data Data stored by the tachograph card that need to be protected for integrity, unauthorised modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data.

Security data The specific data needed to support security enforcing functions (e.g. crypto keys).

System Equipment, people or organisations involved in any way with the recording equipment.

User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE (when not used in the expression 'user data').
User data	Sensitive data stored in the tachograph card, other than security data. User data include identification data and activity data.
Identification data	Identification data include card identification data and cardholder identification data.
Card identification data	User data related to card identification as defined by requirements 190, 191, 192, 194, 215, 231 and 235.
Cardholder identification data	User data related to cardholder identification as defined by requirements 195, 196, 216, 232 and 236.
Activity data	Activity data include cardholder activities data, events and faults data and control activity data.
Cardholder activities data	User data related to the activities carried by the cardholder as defined by requirements 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 and 237.
Events and faults data	User data related to events or faults as defined by requirements 204, 205, 207, 208 and 223.
Control activity data	User data related to law enforcement controls as defined by requirements 210 and 225.

2.3. References U.K.

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991
IC PP	Smartcard Integrated Circuit Protection Profile — version 2.0 — issue September 1998. Registered at French certification body under the number PP/9806
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile — version 2.0 — issue June 99. Registered at French certification body under the number PP/9911

3. Product Rationale U.K.

3.1. Tachograph card description and method of use U.K.

A tachograph card is a smart card, as described in (IC PP) and (ES PP), carrying an application intended for its use with the recording equipment.

The basic functions of the tachograph card are:

- to store card identification and card holder identification data. These data are used by the vehicle unit to identify the cardholder, provide accordingly functions and data access rights, and ensure cardholder accountability for his activities,
- to store cardholder activities data, events and faults data and control activities data, related to the cardholder.

A tachograph card is therefore intended to be used by a card interface device of a vehicle unit. It may also be used by any card reader (e.g. of a personal computer) which shall have full read access right on any user data.

During the end-usage phase of a tachograph card life cycle (phase 7 of life-cycle as described in (ES PP)), vehicle units only may write user data to the card.

The functional requirements for a tachograph card are specified in Annex I B body text and Appendix 2.

3.2. Tachograph card life cycle U.K.

The tachograph card life cycle conforms to smart card life cycle described in (ES PP).

3.3. Threats U.K.

In addition to the smart card general threats listed in (ES PP) and (IC PP), the tachograph card may face the following threats:

3.3.1. Final aims U.K.

The final aim of attackers will be to modify user data stored within the TOE.

T.Ident_Data A successful modification of identification data held by the TOE (e.g. the type of card, or the card expiry date or the cardholder identification data) would allow a fraudulent use of the TOE and would be a major threat to the global security objective of the system.

T.Activity_Data A successful modification of activity data stored in the TOE would be a threat to the security of the TOE.

T.Data_Exchange A successful modification of activity data (addition, deletion, modification) during import or export would be a threat to the security of the TOE.

3.3.2. Attack paths U.K.

TOE's assets may be attacked by:

— trying to gain illicit knowledge of TOE's hardware and software design and especially of its security functions or security data. Illicit knowledge may be gained though attacks to designer or manufacturer material (theft, bribery, …) or through direct examination of the TOE (physical probing, inference analysis, …),

— taking advantage of weaknesses in TOE design or realisation (exploit errors in hardware, errors in software, transmission faults, errors induced in TOE by environmental stress, exploit weaknesses of security functions such as authentication procedures, data access control, cryptographic operations, …),

— modifying the TOE or its security functions through physical, electrical or logical attacks or combination of these.

3.4. Security Objectives U.K.

The main security objective of the entire digital tachograph system is the following:

O.Main The data to be checked by control authorities must be available and reflect fully and accurately the activity of controlled drivers and vehicles in terms of driving, work, availability and rest period and in terms of vehicle speed.

Therefore the main security objectives of the TOE, contributing to this global security objective are the following:

O.Card_Identification_Data The TOE must preserve card identification data and cardholder identification data stored during card personalisation process,

O.Card_Activity_Storage The TOE must preserve user data stored in the card by vehicle units.

3.5. Information technology security objectives U.K.

In addition to the smart card general security objectives listed in (ES PP) and (IC PP), the specific IT security objectives of the TOE that contributes to its main security objectives during its end-usage life-cycle phase are the following:

O.Data_Access	The TOE must limit user data write access rights to authenticated vehicle units,
O.Secure_Communications	The TOE must be able to support secure communication protocols and procedures between the card and the card interface device when required by the application.

3.6. Physical, personnel or procedural means U.K.

The physical, personnel or procedural requirements that contribute to the security of the TOE are listed in (ES PP) and (IC PP) (chapters security objectives for the environment).

4. Security enforcing functions U.K.

This paragraph refines some of the permitted operations such as assignment or selection of (ES PP) and provides additional SEF functional requirements.

4.1. Compliance to protection profiles U.K.

The TOE shall comply with (IC PP).

The TOE shall comply with (ES PP) as refined further.

4.2. User identification and authentication U.K.

The card must identify the entity in which it is inserted and know whether it is an authenticated vehicle unit or not. The card may export any user data whatever the entity it is connected to, except the control **[**[F3]and the company card**]** which may export card holder identification data to authenticated vehicle units only (such that a controller is ensured that the vehicle unit is not a fake one by seeing his name on display or printouts).

Textual Amendments

F3 Inserted by Commission Regulation (EC) No 432/2004 of 5 March 2004 adapting for the eighth time to technical progress Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport (Text with EEA relevance).

4.2.1. User identification U.K.

Assignment (FIA_UID.1.1) *List of TSF mediated actions*: none.

[[X1]**Assignment** (FIA_ATD.1.1) *List of security attributes*:

Editorial Information

X1 Substituted by Corrigendum to Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport (Official Journal of the European Communities L 207 of 5 August 2002).

USER_GROUP	:	VEHICLE_UNIT, NON_VEHICLE_UNIT,
USER_ID	:	Vehicle Registration Number (VRN) and registering Member State code (USER_ID is known for USER_GROUP = VEHICLE_UNIT only).**]**

4.2.2. User authentication U.K.

Assignment (FIA_UAU.1.1) *List of TSF mediated actions*:

— Driver and Workshop cards: export user data with security attributes (card data download function),

— Control card: export user data without security attributes except cardholder identification data.

Authentication of a vehicle unit shall be performed by means of proving that it possesses security data that only the system could distribute.

Selection (FIA_UAU.3.1 and FIA_UAU.3.2): prevent.

Assignment (FIA_UAU.4.1) *Identified authentication mechanism(s)*: any authentication mechanism.

The Workshop card shall provide an additional authentication mechanism by checking a PIN code (This mechanism is intended for the vehicle unit to ensure the identity of the card holder, it is not intended to protect workshop card content).

4.2.3. Authentication failures U.K.

[F4Additionally the following assignments describe the card reaction for each single user authentication failure.

Textual Amendments

F4 Substituted by Commission Regulation (EC) No 432/2004 of 5 March 2004 adapting for the eighth time to technical progress Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport (Text with EEA relevance).

Assignment (FIA_AFL.1.1) *Number*: 1, *list of authentication events*: authentication of a card interface device.

Assignment (FIA_AFL.1.2) *List of actions*:

— warn the entity connected,

— assume the user as NON_VEHICLE_UNIT.

Additionally the following assignments**]** describe the card reaction in the case of failure of the additional authentication mechanism required in UIA_302.

Assignment (FIA_AFL.1.1) *Number*: 5, *list of authentication events*: PIN checks (workshop card).

Assignment (FIA_AFL.1.2) *List of actions*:

— warn the entity connected,

— block the PIN check procedure such that any subsequent PIN check attempt will fail,

— be able to indicate to subsequent users the reason of the blocking.

4.3. Access control U.K.

4.3.1. Access control policy U.K.

During end-usage phase of its life cycle, the tachograph card is the subject of one single access control security function policy (SFP) named AC_SFP.

Assignment (FDP_ACC.2.1) *Access control SFP*: AC_SFP.

4.3.2. Access control functions U.K.

Assignment (FDP_ACF.1.1) *Access control SFP*: AC_SFP.

Assignment (FDP_ACF.1.1) *Named group of security attributes*: USER_GROUP.

Assignment (FDP_ACF.1.2) *Rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*:

[F4GENERAL_READ: User data may be read from the TOE by any user, except cardholder identification data which may be read from control cards and company cards by VEHICLE_UNIT only.**]**
IDENTIF_WRITE : Identification data may only be written once and before the end of phase 6 of card's life-cycle. No user may write or modify identification data during end-usage phase of card's life-cycle.
ACTIVITY_WRITE: Activity data may be written to the TOE by VEHICLE_UNIT only.
SOFT_UPGRADE : No user may upgrade TOE's software.
FILE_STRUCTURE: Files structure and access conditions shall be created before end of phase 6 of TOE's life-cycle and then locked from any future modification or deletion by any user.

4.4. Accountability U.K.

The TOE shall hold permanent identification data.

There shall be an indication of the time and date of the TOE's personalisation. This indication shall remain unalterable.

4.5. Audit U.K.

The TOE must monitor events that indicate a potential violation of its security.

Assignment (FAU_SAA.1.2) Subset of defined auditable events:

- — cardholder authentication failure (5 consecutive unsuccessful PIN checks),
- — self test error,
- — stored data integrity error,
- — activity data input integrity error.

4.6. Accuracy U.K.

4.6.1. Stored data integrity U.K.

Assignment (FDP_SDI.2.2) *Actions to be taken*: warn the entity connected,

4.6.2. Basic data authentication U.K.

Assignment (FDP_DAU.1.1) *List of objects or information types*: activity data.

Assignment (FDP_DAU.1.2) *List of subjects*: any.

4.7. Reliability of service U.K.

4.7.1. Tests U.K.

Selection (FPT_TST.1.1): during initial start-up, periodically during normal operation.

Note: during initial start-up means before code is executed (and not necessarily during Answer To Reset procedure).

The TOE's self tests shall include the verification of the integrity of any software code not stored in ROM.

Upon detection of a self test error the TSF shall warn the entity connected.

After OS testing is completed, all testing-specific commands and actions shall be disabled or removed. It shall not be possible to override these controls and restore them for use. Command associated exclusively with one life cycle state shall never be accessed during another state.

4.7.2. Software U.K.

There shall be no way to analyse, debug or modify TOE's software in the field.

Inputs from external sources shall not be accepted as executable code.

4.7.3. Power supply U.K.

The TOE shall preserve a secure state during power supply cut-off or variations.

4.7.4. Reset conditions U.K.

If power is cut (or if power variations occur) from the TOE, or if a transaction is stopped before completion, or on any other reset conditions, the TOE shall be reset cleanly.

4.8. Data exchange U.K.

4.8.1. Data exchange with a vehicle unit U.K.

The TOE shall verify the integrity and authenticity of data imported from a vehicle unit.

Upon detection of an imported data integrity error, the TOE shall:
— warn the entity sending the data,
— not use the data.

The TOE shall export user data to the vehicle unit with associated security attributes, such that the vehicle unit will be able to verify the integrity and authenticity of data received.

4.8.2. Export of data to a non-vehicle unit (download function) U.K.

The TOE shall be able to generate an evidence of origin for data downloaded to external media.

The TOE shall be able to provide a capability to verify the evidence of origin of downloaded data to the recipient.

The TOE shall be able to download data to external storage media with associated security attributes such that downloaded data integrity can be verified.

4.9. Cryptographic support U.K.

If the TSF generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes. Generated cryptographic session keys shall have a limited (TBD by manufacturer and not more than 240) number of possible use.

If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods.

5. Definition of security mechanisms U.K.

Required security mechanisms are specified in Appendix 11.

All other security mechanisms are to be defined by the TOE manufacturer.

6. Claimed minimum strength of mechanisms U.K.

The minimum strength of mechanisms for the Tachograph Card is *High* as defined in (ITSEC).

7. Level of Assurance U.K.

The target level of assurance for the Tachograph Card is ITSEC level *E3*, as defined in (ITSEC).

8. Rationale U.K.

The following matrixes give a rationale for the additional SEFs by showing:

— which SEFs counteract which threats,

— which SEFs fulfil which IT security objectives.

	Threats											**IT Objectives**								
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
UIA_301 Authentication means																			x	
UIA_302 PIN checks																			x	
ACT_301 Identification data																				
ACT_302 Personalisation date																				
RLB_301 Software integrity												x		x						
RLB_302 Self tests												x		x						
RLB_303 Manufacturing tests					x	x						x		x						
RLB_304 Software analysis					x		x	x				x		x						
RLB_305 Software input					x	x		x				x		x						
RLB_306 Power supply									x	x		x		x						

RLB_307 Reset												x		x						
DEX_301 Secured data import											x									x
DEX_302 Secured data import											x									x
DEX_303 Secured data export to VU											x									x
DEX_304 Evidence of origin											x									x
DEX_305 Evidence of origin											x									x
DEX_306 Secured export to external media											x									x
CSP_301 key generation												x								x
CSP_302 key distribution												x								x]]